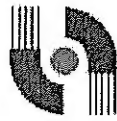


MULTIMEDIA



UNIVERSITY

STUDENT ID NO

--	--	--	--	--	--	--	--	--	--

# MULTIMEDIA UNIVERSITY

## FINAL EXAMINATION

TRIMESTER 1, 2019/2020

### TAC3121 – APPLIED CRYPTOGRAPHY

(All Sections / Groups)

18 OCTOBER 2019

3.00 p.m. – 5.00 p.m.

(2 Hours)

---

#### INSTRUCTIONS TO STUDENT

1. This Question paper consists of 3 pages with 5 Questions only.
2. Attempt **ALL** questions. All questions carry equal marks (10 marks) and the distribution of the marks for each question is given.
3. Please print all your answers in the Answer Booklet provided.

**Question 1**

- 1a) Describe the importance of providing data security with any **FOUR** examples. [4 marks]
- 1b) What is the difference between an unconditionally secure cipher and a computationally secure cipher? [4 marks]
- 1c) State the **TWO (2)** requirements for the secure use of symmetric encryption. [2 marks]

**Question 2**

- 2a) Perform the following operations using modulo reduction. [4 marks]
- i.  $(4223 + 17323) \bmod 10$   
ii.  $(221 \times 23) \bmod 22$
- 2b) Using Euler's Totient function, find the value of [4 marks]
- i.  $\phi(29)$  ii.  $\phi(80)$
- 2c) Using the Rail Fence cipher of depth 2, decipher the following: [2 marks]

**WAEONUCEERBRTSCED**

**Question 3**

- 3a) Identify the plaintext for the following ciphertext: [4 marks]

**ERMBOSTPSLTIEZPESLNTSPIAUTZZ**

Assume the usage of single stage keyed columnar transposition cipher and the decryption key as  $(3 \ 1 \ 4 \ 2)$

- 3b) Given that Bob has public RSA key  $e = 3$  and  $p=11, q=3$ . Compute Bob's private key  $d$ . [3 marks]
- 3c) State **ONE (1)** similarity and **TWO (2)** differences between a message authentication function (MAC) and a one-way hash function. [3 marks]

Continued...

**Question 4**

- 4a) Explain triple DES with two keys with a diagram. [2 marks]
- 4b) Explain **TWO (2)** advantages and **TWO (2)** security issues of Electronic Code Book (ECB) mode of operation. [4 marks]
- 4c) Explain the use of message authentication code (MAC) to provide both authentication and confidentiality when "*authentication is tied to plaintext*" with a diagram. [4 marks]

**Question 5**

- 5a) Explain **TWO (2)** types of attacks addressed by digital signature. [2 marks]
- 5b) Users A and B use the Diffie-Hellman key exchange technique with a common  $q=71$  and a primitive root  $a=7$ . [4 marks]
- i. If user A has private key  $X_A = 5$ , what is A's public key  $Y_A$ ?
  - ii. If user B has private key  $X_B = 12$ , what is B's public key  $Y_B$ ?
  - iii. What is the shared secret key,  $K$ ?
- 5c) Describe **FOUR (4)** components of public-key certificates. [4 marks]

**End of Paper**